04

Effectiveness of Police Training in Cybercrime Incident Response Within the Directorate of Criminal Investigations, Kenya

Mercy Jepleting, Stephen Olala, and Irene Mwingirwa

Abstract

In recent years, addressing cybercrime has become a top priority for police organisations. Ensuring that police officers possess the necessary skills and knowledge to respond effectively to cybercrime is a primary concern. Conducted at DCI headquarters, this study, grounded in structural contingency theory, aimed to assess the adequacy of police training in responding to cybercrime incidents. The research employed a mixed methodology, with 133 respondents chosen through stratified random and purposive sampling. Data was collected by use of questionnaires and interview schedules and analysed using qualitative and quantitative methods. The findings revealed that many respondents emphasised the importance of personal cybersecurity in investigating cybercrime incidents in Kenya. Victims often lacked knowledge of comprehensive cybersecurity measures and behavior monitoring was identified as essential in responding to cybercrimes. The analysis highlighted a lack of emphasis on digital crime training within the DCI. This indicates insufficient training in responding to cybercrime incidents. In light of these findings, this study recommends several actions to enhance police training on cybercrime. These include assessing officers' qualifications, employing cybersecurity specialists, collaborating with local and international partners for training and information sharing, continuous training on the latest cybercrime techniques, promoting citizen cybersecurity awareness, and allocating adequate budget for cybercrime incident response training programs.

Keywords: Cybercrime incident response, police training adequacy, competencies, policing preparedness and training

Introduction

Police agencies are becoming increasingly burdened by cybercrime difficulties (Loveday, 2017; Wydra, 2015). They must therefore react and strengthen their readiness to combat cybercrime as it continues to rise in "frequency, scale, sophistication, and severity" (Antrobus, 2019). Much of the literature to date focus on the different ways in which police organisations are currently ill-equipped or finding it difficult to enhance their overall ability to handle citizen assistance requests or carry out more successful investigations and prosecutions of cyber criminals (Harkin et al., 2018; Leppanen et al., 2016). Although the need for improved "training" has been amply demonstrated, there has not been as much discussion about who needs this training explicitly, how it should be delivered, or what specific issues it should be trying to address. In light of this, this research investigates the issues raised by a lack of training.

Specialist cyber units carry out formal and informal "border-spanning" (Harichandran et al., 2016) tasks vertically and horizontally. These tasks include giving strategic advice to police executives regarding present and future challenges of cybercrime and operational advice to field general investigators and other specialist units concentrating on technical crimes. Therefore, this study aimed to assess the adequacy of police training on cybercrime incident response within the Directorate of Criminal Investigations, Kenya.

Statement of the problem

Police organisations must give law enforcement professionals cybercrime training to ensure local law enforcement authorities are ready to battle cybercrime. Despite the difficulties that law enforcement organisations encounter in deploying officers to locally combat computer crime, cybercrime training equips law enforcement personnel with the ability to respond to the crimes appropriately (Cockcroft et al., 2021). This underlines the need for law enforcement personnel to be trained in cybercrime-related incidents to assist in crime investigation, locate a suspect, and make an arrest. However, most of these organisations lack the expertise needed to properly investigate cybercrimes since officer training emphasises conventional methods, which are ineffective in dealing with the landscape of cybercrime (Cunha et al., 2017). As a result, law enforcement agencies have shown resistance to investing in the fight against cybercrime (Graham et al., 2020). According to Amber's 2023 report, there was a significant surge in cyber-attacks across Kenya of upto 76% between 2018 and 2023. Of particular concern is the emergence of exploits as the predominant method of attack (Amber, 2023). This alarming rise in cyber incident responses underscores the urgent need for a comprehensive analysis of cybercrime incident response within the DCI. In order to unravel this scenario and bring more impetus to address this problem, this study sought to assess the adequacy of police training in cybercrime incident response in Kenya.

Objective of the study

The general objective of the study was to assess the adequacy of police training in cybercrime incident response in Kenya.

Significance of the study

The findings and recommendations derived from this study have significant implications on various fronts. They can guide policy makers in formulating strategic cybercrime policies and legislation to enhance cybercrime response and e-policing in Kenya. These findings contribute to the knowledge about cybercrime incident responses in the country, providing a foundation for future research and initiatives to combat cyber threats. Moreover, the findings of the study can initiate scholarly debates on the preparedness of law enforcement units in developing countries to handle cybercrime-related incident responses.

Scope and limitations

This study focused on evaluating the adequacy of police training in cybercrime incident response in Kenya. Nevertheless, the study incorporated these peripheral aspects into its recommendations for action. The limitations during the study included potential hesitation among respondents for fear of victimisation or concerns about the vulnerability of the information to manipulation. Participants' confidentiality was assured, though some had limited access to cybercrime information in Kenya. They were also reassured that their data would not be shared with third parties.

Literature review

Cybercrime concerns are putting a growing strain on police organisations (Harkin et al., 2018; Holt & Bossler, 2019; Willits & Nowacki, 2016). Police agencies should therefore react and strengthen their readiness to combat cybercrime as it continues to rise in "frequency, scale, sophistication, and severity" (Australian Cyber Security Centre, 2017: 16).

Research consistently emphasises the necessity for more or better training in technical understanding of cyber-offending. The ineffectiveness of current training and the need for clearer training for all officers are described by Hadlington et al. (2018); educational and training programmes to improve the views of constables are suggested by Holt, Burruss, and Bossler (2019); several concerns regarding the effectiveness of existing training arrangements in facilitating the development of cyber skills within police officers are detailed by Cockcroft et al. (2018); and Harkin et al. (2018) suggest that broader training and up-skilling are necessary. Research by Schreuders et al (2020) also suggests that there was a lack of structured or formalised training and that this impeded effective practice; and official policy documents often make reference to the need for improved 'capabilities' including 'digital training for investigators' or training in 'general digital awareness' (Hitchcock et al., 2017; Home Affairs Committee, 2018).

In this subject, it is typical for academic writing or policy materials to highlight the necessity of better training. It will be argued, based on the opinions of cyber-crime unit members, that inadequate training is likely to cause issues for four different categories of police workers: (a) frontline officers who perform generalist duties in their communities; (b) upper management who hold positions of authority over organisational policy and strategic decision-making; (c) general investigators in their communities or in various other areas of police organisations, as well as low-skilled investigators working in specialised cyber-crime units; and (d) highly skilled specialist cyber-crime unit investigators and digital forensic analysts who are performing the most technically-sophisticated forms of police investigation and inquiry. Each of these groups face unique training challenges.

In other words, lack of training appears very different for a frontline officer compared to the demands placed on a digital forensic analyst. These groups face different challenges and strategic approaches to redress these problems must be cognizant of how to respond to their unique situational needs. Recognising these differences will shape approaches for strengthening how the broader police organisation can better respond to cyber-crime and advance the literature beyond simply suggesting that 'more and better training is needed'.

Empirical literature review gaps

With just few empirical studies, literature on police responses to cybercrime is still under-developed (Willits & Nowacki, 2016), although it is expanding (Bossler, 2012). However, lack of training has frequently been mentioned as a concern (Leukfeldt et al., 2017). According to Cockcroft et al. (2018), the wider field and the habitus of non-specialist officers will continue to fail to recognise its importance if cyber knowledge remains the domain of police specialists. This research concurs but points out that there are probably many unknowns and that the risks go far beyond. The current study tries to demonstrate how lack of training is probably relative to various police units and how, depending on the group in question, it causes different issues. Specialists, frontline officers, upper management, and general investigators deal with particular situations that build upon and interact with one another. Future initiatives to enhance police proficiency and increase their ability to combat cybercrime must consider these varying training requirements. In the foreseeable future, specialised cybercrime units will probably be crucial and significant. However, through focused training, the skill gaps that separate them from the rest of the company will be filled.

Theoretical framework

The study was guided by Structural Contingency Theory.

Structural contingency theory

The mechanics of conventional crimes committed online continue to complicate how local, state, and federal law enforcement organisations manage cybercrime investigations. In the past, law enforcement organisations have been in charge of conducting investigations into cybercrimes (Brunner, 2020). However, state authorities have stressed the necessity of solving the issues associated with cybercrime in order to decrease future computer crimes. Structural contingency theory was applied to the study to comprehend the impact and function of law enforcement organisations in dealing with local cybercrimes. Lawrence and Lorsch (1967) tried to understand how organisations might change to satisfy their immediate environmental needs.

In addition, Lawrence and Lorsch's strategy contributes to understanding police organisational behaviours related to capacity of law enforcement agencies to respond to cybercrime. This is a critical factor in how organisations allocate resources (Matusiak, 2019). How law enforcement organisations respond to cybercrimes sends a clear message to people and businesses about the agency's priorities for combating cybercrime, which may impact how people report cybercrimes.

Police agencies modify their organisational strategies in response to changing environmental conditions to address their areas of concern (Donaldson, 2001). To put it another way, police chiefs in law enforcement agencies alter the organisational structure to optimise their objectives for the success of the agency (Matusiak, 2019). Furthermore, the contingency theory is relevant to cyber policing because, as threats become more common and expensive for society, local police departments will probably commit more training resources to investigate cybercrimes.

Methodology

The study adopted a descriptive design guided by qualitative and quantitative research techniques. The Directorate of Criminal Investigations Headquarters, located on the outskirts of Nairobi, served as the research site. The DCI has eight formations: Ballistics Unit, Forensics Department, Cybercrime Unit, Anti-Banking Fraud Unit, Serious Crimes Unit, Anti-Narcotics Unit, Special Crime Prevention Unit, and Land Fraud Unit. The choice of the DCI facilitated an in-depth exploration of the multifaceted realm of cybercrime investigation in Kenya. The target population of the study, according to DCI Human Resource Report of 2021 were 200 commissioned officers, non-commissioned officers, gazetted, and police constables. The study employed a stratified random and purposive sampling approaches. The sample size of the study were 133 respondents derived using Yamane (1967) formula as indicated in Table 4.1.

TABLE 4.1 ◢ Sample size

Category	Target population	Sample size	Sample (%)
Assistant Superintendent	7	5	66.5
Chief Inspector	9	6	66.5
Inspector	16	11	66.5
Senior Sergeant	25	16	66.5
Sergeant	35	23	66.5
Corporal	43	29	66.5
Constable	65	43	66.5
Total	**200**	**133**	

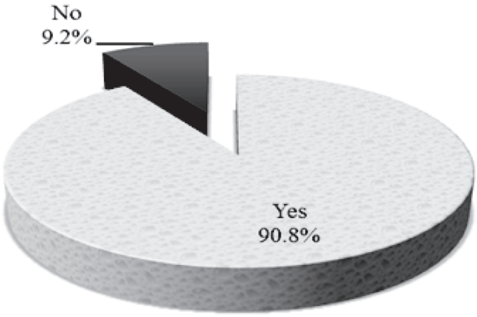
Source: Directorate of Criminal Investigations Human Resource Report (2021)

The principal means of data acquisition was a semi-structured questionnaire. This instrument served as the primary tool for gathering information. It explicitly targeted individuals at the rank of Senior Sergeant down to those occupying the position of Police Constables. The study incorporated secondary data from empirical references, periodicals, academic journals, books, and policy documents related to cybercrime. The data played a crucial role in substantiating the findings derived from primary data. Statistical Package for Social Sciences (SPSS) version 26 was used to analyse quantitative data and the findings were presented in form of tables and figures. Qualitative data was presented thematically and in narratives.

Findings

Figure 4.1 illustrates that Some 90.8% of the participants concurred that the training of police officers has a significant impact on the handling of cybercrime incident responses. The respondents highlighted the importance of cybercrime training in areas like recovery, prevention, deterrence, processing, preservation, and prosecution. This is consistent with the views of scholars like Holt and Bossler (2015) who stress the pivotal role of training in enhancing capabilities for cybercrime investigation.

FIGURE 4.1 ◢ Police officers' training adequacy on cybercrime incident response



Forms of police training on cybercrime incident response

Table 4.2 indicates that the study identified various forms of police training as follows: forensics toolkits (40.62%), online behaviour monitoring (22.92%), and surveillance techniques (10.42%). These findings underscore the diverse training needs in cybercrime investigation, as supported by scholars like Holt and Bossler (2015). During interviews one of R-CIR (Respondent on Cybercrime Incident Response) noted as follows:

> *Providing digital forensics investigation requires high standards of training. Our police officers are not in a position to assist the victims of cybercrime since the majority of them are not properly trained in cybercrime related certifications and accreditations. Majority of the reported cases are yet to be concluded. However, the DCI is making significant attempts to professionalise the cybercrime investigation unit through international multi-agency partnership with Federal Bureau of Investigations (FBI) and leading cyber forensics firms in the country.*

In another interview, one of the officers from the R-CIRM (Cybercrime Incident Response Management) opined that:

> *Due to the threat which cybercrime poses to the various facets of the society, the importance of trained prosecutors and investigators who are very conversant with cyber forensics is turning out to be pivotal, since most of the criminal acts are*

nowadays committed through online platforms. In order to match the changing and demanding needs of cybercrime investigations, the investigators require both hard and soft skills.

TABLE 4.2 ◢ Forms of police training on cybercrime incident response

Form of training	Frequency	Percentage (%)
Forensics toolkits	39	40.62
Retrieving of files	14	14.58
Awareness training	11	11.45
Online behaviour monitoring	22	22.92
Surveillance techniques	10	10.42
Total	**96**	**100**

From the interviews, respondents unveiled several areas of concern in police training that need improvement to enhance the effectiveness of cybercrime incident response and investigations in the country. These areas include:

- Understanding the various forms and impact of cybercrime;
- Enhancing general awareness of cybercrimes and staying informed about emerging trends;
- Developing expertise in preserving digital evidence, particularly on mobile devices;
- Providing additional training and knowledge in digital technology, including increasing frontline awareness of technology usage and current applications;
- Enhancing training in sourcing digital evidence and gathering cybercrime intelligence;
- Offering more training on Open-Source Intelligence (OSINT), Big Data analytics, Artificial Intelligence, and Machine Learning in the context of cybersecurity; and
- Providing comprehensive training in forensics output examinations for officers.

Leading training areas enabling adequate cybercrime response

The research sought to identify key training areas crucial for responding to cybercrime incidents. The findings revealed that 65.63% highlighted the importance of prioritising personal cybersecurity as one of the primary components of managing cybercrime within the DCI. In addition, 9.38%

mentioned the significance of education ,while 6.25% emphasised the need for awareness training and behavior monitoring. Furthermore, 12.5% participants noted the importance of online surveillance techniques. This includes monitoring suspicious accounts, analysing questionable transactions, and visualising money flows and cases. The findings are presented in Table 4.3.

TABLE 4.3 ◢ Leading training mechanism which enables adequate cybercrime

Training mechanism	Frequency	Percentage (%)
Emphasis on personal cyber security	63	65.63
Education	9	9.38
Awareness training	6	6.25
Behaviour monitoring	6	6.25
Surveillance	12	12.5
Total	**96**	**100**

Effect of police officers' training and skills on cybercrime incident response

The study found that 40.63 % of respondents agreed to a higher extent that the level of police officers' training and skills affected cybercrime incident response in Kenya. Further, 26.04% indicated a medium extent, 20.83% cited a small extent, and 12.5% indicated no extent. The findings are summarised in Table 4.4.

TABLE 4.4 ◢ Police officers' training and skills extent on cybercrime incident response

Training mechanism	Frequency	Percentage (%)
High extent	39	40.63
Medium extent	25	26.04
Small extent	20	20.83
No extent	12	12.5
Total	**96**	**100**

During interviews, one of the R-CIM officers noted that:

> *The DCI level of training and skills on cybercrime is quite basic. Majority of them are trained in dealing with physical criminal acts and have less knowledge on technical crimes. Most of the reported cases on cybercrimes are never conclusively handled by the DCI and the entire NPS fraternity. Majority of these cases are conducted through*

> *relying on network service providers such as Safaricom and experts in cybercrimes within the financial industry. The DCI needs to have regional offices entirely tasked with cybercrime-related incident responses.* (R-CIM02)

Summary of findings

The study found that providing officers with the most recent cybercrime training should be the top priority in order to increase their understanding of cybercrime investigation and prevention. Yet, law enforcement agencies lacked the necessary training and technology to apprehend and compete with cyber criminals. There was little push for local law enforcement to undertake cybercrime training. The two critical aspects in officer training include educating officers about identifying suspicious emails and providing in-service training that encompasses the essentials of recognising cybercrime threats in the current landscape.

Conclusion

The study concludes that training levels are a common issue among the DCI units, and hence the need to review training infrastructure to confront digital and cyber-related offences. Whearas other empirical data also seem to point to this problem, the results of this investigation show that it is indeed a substantive problem. In particular, the challenge of adequately trained police officers on cybercrime investigations is critical. This shows that the DCI had a challenge in responding to cybercrime incidents due to training deficiencies. The study also indicates that technical knowledge is a significant challenge when responding to cybercrimes. The findings of the study imply a need for an increase in cybercrime training budget among the police to ensure that law enforcement officers are prepared to deal with emerging cybercrime trends. The study noted that the existing police training curriculum lacked basic cybercrime training. This makes it a significant challenge for the victims of cybercrimes since the police are not in a position to guarantee the successful prosecution of the perpetrators.

Recommendations

The study makes the following recommendations:

i The DCI should regularly review of the cybercrime curriculum to respond to the changing threat landscape.

ii DCI should regularly evaluate the qualifications of its cybercrime officers, considering their education in fields like computer science and digital forensics, and assessing specialised training in cybercrime investigations. Experts should be selected based on their qualifications and relevant knowledge.

iii The National Police Service through the DCI should collaborate with the DCI, other agencies, and the private sector to harness knowledge and skills that are critical to investigation of complicated cybercrimes.

iv The DCI should allocate budget to cybercrime training of its officers. Adequate funding ensures that training programmes are well- resourced and can provide high-quality training opportunities.

References

Amber, J. (2023). Cyberattack in Kenya impacts online government platforms: cybermagazine. https://cybermagazine.com/application-security/cyber-attack-in-kenya-impacts-online-government-platforms

Australian Cyber Security Centre (2017) *ACSC Threat Report 2017*. Retrieved from: https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

Bossler, A.T. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management 35*(1): 165–181.

Brunner, M. (2020). Challenges and opportunities in state and local cybercrime enforcement. *Journal of National Security Law & Policy, 10*(3), 1.

Cockcroft, T., Shan-A-Khuda, M., Schreuders, C., & Trevorrow, P. (2018) Police cybercrime training: Perceptions, pedagogy, and policy. *Policing: A Journal of Policy and Practice*. Online first.

Cunha, I., Cavalcante, J., & Patel, A. (2017). A proposal for curriculum development of educating and training Brazilian police officers in digital forensics investigation and cybercrime prosecution. I*nternational Journal of Electronic Security and Digital Forensics, 9*(3), 209.

Donaldson, L. (2001). *The contingency theory of organizations* (1st ed.). SAGE Publications.

Graham, A., Kulig, T. C., & Cullen, F. T. (2020). Willingness to report crime to the police. *Policing: An International Journal*, 43(1), 1–16.

Hadlington, L, Lumsden K, Black A, and Ferra F (2018) A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice*. Online first.

Harichandran, V.S., Breitinger, F., Baggili, I. and Marrington, A., (2016) Cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security, 57*, pp.1-13.

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Practice and Research 19*(6): 519-536.

Hitchcock, A., Holmes, R. & Sundorph, E. (2017) *Bobbies on the net: a police workforce for the digital age*. London: Reform.

Holt, T., & Bossler, A. (2015). *Cybercrime in Progress: Theory and prevention of technology-enabled offences* (1st ed.). Routledge. https://doi.org/10.4324/9781315775944

Holt, T., Burruss, G., & Bossler, A. (2019) An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents. *Policing and Society 29*(8): 906-921.

Home Affairs Committee (2018) *Policing for the future: Tenth report of session 2017-19*. London: House of Commons.

Koziarski, J., & Lee, J. (2020). Connecting evidence-based policing and cybercrime. P*olicing: An International Journal, 43*(1), 198–211.

Lawrence, P. R., & Lorsch, J. W. (1967). Differentiation and integration in complex organizations. *Administrative Science Quarterly, 12*(1), 1.

Leppanen, A., Kiravuo, T., & Kajantie, S. (2016). Policing the cyber-physical space. *The Police Journal: Theory, Practice and Principles, 89*(4), 290–310.

Leukfeldt, R., Veenstra, S., & Stol, W. (2017). High volume cybercrime and the organization of the police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology, 7*(1), 1–17.

Loveday, B. (2017). 'Still plodding along? The police response to the changing profile of crime in England and Wales'. *International Journal of Police Science & Management, 19*(2), pp.101-109.

Matusiak, M. C. (2019). Environmental predictors of municipal police agency goals. *Police Quarterly, 22*(1), 112–136.

Schreuders C, Cockcroft T, Butterfield E, Elliott J, Ryad Soobhany A, and Shan-A-Khuda M (2020) Needs assessment of cybercrime and digital evidence in a UK police force. *International Journal of Cyber Criminology* 14(1): 316-340.

Willits, D. & Nowacki, J. (2016). The use of specialised cybercrime policing units: An organisational analysis. *Criminal Justice Studies* 29(2): 105–24.

Wydra, C. (2015). 'Educating the Technology Officer of the Future: A Needs Analysis.' *Issues in Information Systems*, 16(4): 224-231.

Yamane, T. (1967). *Statistics: An Introductory Analysis*, 2nd Ed., New York: Harper and Row.